STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Network Server Security

Product ID: ENT-SEC-022

Effective Date: October 2004

Approved: Steve Bender, Acting Director, Department of Administration

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

A. Scope

This policy applies to all servers that reside on the state's network, including all state agencies as well as local government entities. This policy does not apply to colleges and universities or the Commissioner of Higher Education Office.

B. Purpose

Physical and administrative access to the state network must be controlled to prevent the intentional or unintentional modification, destruction, disclosure, or misuse of data and information resources.

C. Definitions

For the purposes of this policy, the following definitions apply:

Supervisor: The term Supervisor is used as a generic term for whatever userID is actually used on the server for system setup, administration and maintenance. This userID will normally be something such as ADMIN, ADMINISTRATOR, SUPERUSER, SUPERVISOR, ROOT or ACF2ID that has supervisory privileges. This userID is not intended to be used as a normal account because it bypasses **all** security checks, has the ability to create and delete other accounts, and has the ability to give other accounts Supervisor privileges.

Server: A server is a high-speed computer or computer system in a network that is shared by multiple users. The term server may refer to both the hardware and software (the entire computer system) or just the software that performs the services. The term server as used in this policy applies to the following types of servers: application, database, file, intranet, network access, print, remote access, and web servers.

D. Requirements

1. Physical Access

Only personnel authorized to operate a server will have access to the physical area where the server resides. Keys and/or other security devices must be used to secure the physical area and a list of all authorized personnel maintained. In areas with highly secure servers, cleaning and maintenance personnel must be supervised by an authorized user while they are working in the area.

Access to network equipment such as hubs, MAUs, routers, switches, firewalls, bridges, patch panels, gateways, communication servers and the like must be controlled the same as servers. Physical access must be restricted to prevent tampering or accidental disruption of service. Servers and other network equipment must be kept in a locked environment, only accessible by authorized systems support personnel.

It is the responsibility of the agency to provide a secured area to house network equipment and servers. In consideration of external constraints on physical space and the costs to modify some locations, agencies should continue to work with building management to provide this secured area. An agency will submit to the State Information Security Manager positive confirmation of its compliance with this section of the policy and documentation of areas where compliance has not been accomplished. The agency should document its plans to meet the requirements of this policy.

2. Administrative Access

Supervisor level access given to employees must be approved by the Agency Security Officer. Employees having userIDs with Supervisor privileges will be documented including the need for Supervisor access.

3. Audit Log

The use of enterprise Supervisor userIDs must be logged using either an access log or an auditing software package. Anytime CONSOLE or administrative access is gained to an agency server, it must be logged in an access log containing the date, time, network address, user, and a description of what was done and why. Agencies must be notified in advance when anyone outside the agency gains console or administrative access to one of their servers.

Servers handling sensitive, valuable, or critical information must log all significant computer security relevant events. Examples of computer security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, modifications to system software, and administration changes affecting the state network.

Auditing functions will be administered by designated Agency Security Officers. Periodic checks of auditing logs must be completed. Any security violations must be reported to the ITSD Service Desk. Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, security measures. Electronic versions of these logs must be retained for at least 30 days. If paper versions of these logs are printed, they must be retained for at least five (5) years.

The server console or access to administrative areas on the server must be password protected. Servers must be periodically audited for compliance with the existing security policies. These audits must be performed at least once a quarter.

4. Server Updates And Patches

Agencies will ensure that all servers are updated in a timely manner with the latest security patches and updates. In the event of an attack that relates to a patched vulnerability, patches must be installed immediately upon notification or

vulnerable devices will be disconnected from the network until they are properly patched. All other security patches must be installed according to the alert classification documented located on the security topics web site at http://mine.mt.gov/security/View.asp?ID=84

E. Background - History On The Creation Of Or Changes To This Policy

The NetWare Managers Group Policy Committee originally created this policy in 1996. The policy was adopted later that year. The ITSD Security Section modified this policy in January 2002. The policy revisions were reviewed with the Information Technology Managers Council for comment prior to adoption.

ITSD has formed a project team that is working to resolve the physical security issues associated with server and telecommunications equipment (routers, LAN switches, telephone switches, etc.). The project team proposes to conduct an inventory of statewide and agency equipment on the Helena campus, major sites, and remote offices. The project team will then complete a gap analysis and make recommendations to resolve the physical security deficiencies identified through budget proposals and a 5-year implementation plan.

This policy was updated by the State Security Committee in March, 2004 to address auditing software needs.

F. Guidelines - Recommendations, Not Requirements

The area where servers and other network equipment is kept should be designed to withstand hazards such as fire, flooding and natural disasters. The room's heat, ventilation and air conditioning (HVAC) systems must be reliable. Electrical power must be reliable and all critical electronic devices must be powered through uninterruptible power supplies (UPS) correctly sized for running the devices long enough for an automated or manual shutdown of the device.

Also refer to the Physical Access section of the policy for agency reporting responsibilities for compliance purposes.

G. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- 2-17-514(1) – Enforcement
- §2-17-505(2), MCA
- §2-17-512, MCA
- §2-15-114, MCA
- 2-17-512, MCA; 2-17-534, MCA; 2-15-114, MCA; UserID, Password, and Access Policy; LAN Backup and Archiving Plan Policy

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-112, MCA
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 3-0130 Discipline
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-SEC-022
Proponent:	Steve Bender, Acting Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	October 2004
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.